ELSEVIER

Journal of Pure and Applied Algebra 117&118 (1997) 195–215

JOURNAL OF PURE AND APPLIED ALGEBRA

Solving a system of algebraic equations with symmetries[1]

Antoine Colin *

GAGE, Centre de mathématiques (CNRS URA 169), École polytechnique, F-91128 Palaiseau Cedex, France

Abstract

We propose a method to solve some polynomial systems whose equations are invariant by the action of a finite matrix multiplicative group G. It consists of expressing the polynomial equations in terms of some *primary invariants* $\Pi_1,\ldots,\Pi_n$ (e.g., the elementary symmetric polynomials), and one single "primitive" *secondary invariant*. The primary invariants are a transcendence basis of the algebra of invariants of the group G over the ground field k, and the powers of the primitive invariant give a basis of the field of invariants considered as a vector space over $k(\Pi_1,\ldots,\Pi_n)$. The solutions of the system are given as roots of polynomials whose coefficients themselves are given as roots of some other polynomials: the representation of the solutions $(x_1,\ldots,x_n)$ breaks the field extension $k(x_1,\ldots,x_n) : k$ in two parts (or more). © 1997 Published by Elsevier Science B.V.

1991 Math. Subj. Class.: 12-04, 12E12, 12F10, 12Y05, 13-04, 13B02, 13C10, 13H10, 13P10, 14-04, 20B35, 20C10, 20C30, 20C33, 20C40, 20F29

1. Introduction

Let (F) be a system of p polynomial equations $F_i(X_1,\ldots,X_n) \in k[X_1,\ldots,X_n]$ where k is a commutative field. Solving (F) can mean many different things. For the numerical mathematicians it means finding approximated values of the isolated points of the variety defined by (F). Our point of view is computer algebra and we shall not deal here with the numerical mathematician's point of view; we just quote [20], where it is shown how the symmetries can be taken into account in the numerical methods using homotopies.

* E-mail:colin@ariana.polytechnique.fr.

[1] Research supported by the CNRS GDR 1026 (MEDICIS) and the Galois project of MEDICIS.

PII S0022-4049(97)00011-X

In computer algebra, solving (F) is usually meant to be finding a "convenient" system of generators of the ideal $I = (F_1, \ldots, F_p)$, or of any ideal that has the same radical as I (and hence defines the same sub-variety of $\hat{k}^n$, where $\hat{k}$ is an algebraic closure of k). A "convenient" system of generators is usually understood to be a triangular system with degrees as low as possible. Standard bases (see [8, Ch. 2]) are such systems, but they break the symmetries of the system. Yet, Karin Gatermann is working on decreasing the complexity of standard bases by using symmetries (see [9, 10]).

Here, we shall not try to give generators of the ideal I. We shall try to express the points of the variety defined by I in k^n in successive steps, by introducing some intermediate field extensions between k and the extension of k generated by the coordinates of the solutions of (F).

For this, we shall use the symmetries of (F) and express the polynomials F_i of our system (F) as algebraic elements over a transcendental extension of k. The way we express the F_i in terms of other polynomials using the symmetries of (F) can be seen as an application of a more general problem: how to express the invariants of a group in terms of a small number of them, in fact thanks to a primitive element. This idea was developed in [7], where it was used to compute relative resolvents, in computational Galois theory.

Invariant theory is what we begin with, in Section 3. In Section 4, we apply invariant theory to solve algebraic systems with symmetries. Then in Section 5, we compute a few examples using different variants of the method.

2. Preliminaries

2.1. A few definitions

Let k be a commutative field of characteristic zero. Let $n \in \mathbb{N}^*$ be a positive integer, $X_1, \ldots, X_n$ some indeterminates on k, and $\boldsymbol{X} = (X_1, \ldots, X_n)$.

The general linear group $\mathrm{GL}_n(k)$ acts faithfully on the left on $k[\boldsymbol{X}]$ (and $k(\boldsymbol{X})$) as follows: if $A \in \mathrm{GL}_n(k)$ and $P \in k[\boldsymbol{X}]$ (or $P \in k(\boldsymbol{X})$) are given, we define $A.P(\boldsymbol{X}) = P(b_{1,1}X_1 + \cdots + b_{1,n}X_n, \ldots, b_{n,1}X_1 + \cdots + b_{n,n}X_n)$, where $B = A^{-1} = (b_{i,j})_{i,j \in \mathbb{N}_n^*}$. We denote by $\mathrm{Stab}_L(P)$ the stabilizer of an element, or a subset P in a subgroup L of $\mathrm{GL}_n(k)$, and by $L.P$ the L-orbit of P. In particular, the symmetric group $\mathfrak{S}_n$ can be identified to a subgroup of $\mathrm{GL}_n(k)$ by associating the matrix $A_\tau = (\delta_{i,\tau(j)})_{(i,j) \in (\mathbb{N}_n^*)^2}$ (where δ is Kronecker's symbol) to a permutation $\tau \in \mathfrak{S}_n$. By the induced action, $\mathfrak{S}_n$ acts on $k[\boldsymbol{X}]$ and on $k(\boldsymbol{X})$ with $\tau.X_i = X_{\tau(i)}$, $i \in \mathbb{N}_n^* = \{1, \ldots, n\}, \tau \in \mathfrak{S}_n$.

Definition 1. Let G be a subgroup of $\mathrm{GL}_n(k)$. We say that a polynomial $P \in k[\boldsymbol{X}]$ (resp. a fraction $P \in k(\boldsymbol{X})$) is *an invariant of* G if and only if for all $A \in G$, we have $A.P = P$. We denote by $k[\boldsymbol{X}]^G$ (resp. $k(\boldsymbol{X})^G$) the algebra of polynomial (resp. fractional) invariants of G.

If L is another subgroup of $\mathrm{GL}_n(k)$ such that $G \subset L$, P is called a *primitive invariant of G relative to L* if and only if $\mathrm{Stab}_L(P) = G$ (see Proposition 15 for the explanation of this terminology).

Example 2. Let $\boldsymbol{\Sigma} = (\Sigma_1, \ldots, \Sigma_n)$, where $\Sigma_i = \sum_{1 \le j_1 < \cdots < j_i \le n} \prod_{l=1}^{i} X_{j_l}$ for all $i \in \mathbb{N}_n^*$ (elementary symmetric polynomials). Then, $k[\boldsymbol{X}]^{\mathfrak{S}_n} = k[\boldsymbol{\Sigma}]$ and $k(\boldsymbol{X})^{\mathfrak{S}_n} = k(\boldsymbol{\Sigma})$. More generally, if L is a product of symmetric groups $\mathfrak{S}_{n_1} \times \cdots \times \mathfrak{S}_{n_s}$, with $\sum_{j=1}^{s} n_j = n$ and each $\mathfrak{S}_{n_j}$ acting on the indeterminates $X_{n_1+\cdots+n_{j-1}+k}$, $1 \le k \le n_j$, then $k[\boldsymbol{X}]^L = k[\boldsymbol{\Sigma}^{(1)}, \ldots, \boldsymbol{\Sigma}^{(s)}]$ and $k(\boldsymbol{X})^L = k(\boldsymbol{\Sigma}^{(1)}, \ldots, \boldsymbol{\Sigma}^{(s)})$ where for all $j \in \mathbb{N}_s^*$, $\boldsymbol{\Sigma}^{(j)}$ denotes the family $(\Sigma_1^{(j)}, \ldots, \Sigma_{n_j}^{(j)})$ of the elementary symmetric polynomials in the variables $X_{n_1+\cdots+n_{j-1}+k}$, $1 \le k \le n_j$ (see a proof in [12]).

A converse of the result of Example 2 will be found in Corollary 8.

Proposition 3. *For any finite subgroup G of $\mathrm{GL}_n(k)$, $k(\boldsymbol{X})^G$ has transcendence degree n over k, and therefore $k[\boldsymbol{X}]^G$ has Krull dimension n over k.*

Proof. This proposition is well-known; see [17, Proposition 2.1.1] for instance. □

2.2. What is a system with symmetrics?

Let $\hat{k}$ be an algebraic closure of k. Let us consider a system of p, $p \in \mathbb{N}^*$, polynomial equations

$$(F)\colon\ \forall i \in \mathbb{N}_p^*, \quad F_i(X_1, \ldots, X_n) = 0$$

with $F_i \in k[\boldsymbol{X}]$, for all $i \in \mathbb{N}_p^*$. Let us define the ideal $I(F) = (F_1, \ldots, F_p)$ of $k[\boldsymbol{X}]$, its radical $J(F)$, the ideal $\hat{I}(F) = \hat{k} \otimes_k I(F)$ of $\hat{k}[\boldsymbol{X}]$ generated by the polynomials $1 \otimes_k F_i$, and the manifold $V(F)$ defined in $\hat{k}^n$ by $\hat{I}(F)$.

Definition 4. We define the following subgroups of $\mathrm{GL}_n(k)$:

- The *symmetry group* of the system: $G_{(F)} = \bigcap_{i=1}^{p} \mathrm{Stab}_{\mathrm{GL}_n(k)}(F_i)$.
- The *vector space symmetry group* of (F) as the group associated to the vector space $L(F) = \bigoplus_{i=1}^{n} k.F_i$: $G_{L(F)} = \mathrm{Stab}_{\mathrm{GL}_n(k)}(L(F))$.
- The *ideal symmetry group* of (F) as the group associated to the ideal $I(F)$: $G_{I(F)} = \mathrm{Stab}_{\mathrm{GL}_n(k)}(I(F)) = \{A \in \mathrm{GL}_n(k) / \forall P \in I(F),\ A.P \in I(F)\}$.
- The *manifold symmetry group* $G_{V(F)}$ of (F) as the group associated to the radical ideal $J(F)$ of $I(F)$: $G_{V(F)} = \mathrm{Stab}_{\mathrm{GL}_n(k)}(J(F))$.

For each of the different groups G above, we can define the associated permutation group as $\mathfrak{S}_n \bigcap G$. The following obviously holds:

$$G_{(F)} \subset G_{L(F)} \subset G_{I(F)} \subset G_{V(F)}.$$

Instead of solving (F), we could solve any system (F') such that $V(F') = V(F)$ (or $I(F) = I(F')$ if we pay attention to the multiplicities). And we may choose (F') such that $G_{(F')}$ be bigger than $G_{(F)}$ (the more symmetries we have is the best: see Proposition 15). The best we could hope would be $G_{(F')} = G_{V(F)}$.

We shall not deal here with the problem of finding such a system (F'). We just mention the notion of *equivariant*, more general than that of invariant (see [10] or [21]); equivariants can take into account some group action on the image space k^n. *Throughout the following*, the system (F) is given; and as symmetries, we shall consider the permutations of a fixed finite subgroup G of $G_{(F)}$.

3. Description of the invariants of a group

Here we describe the algebra of the invariants of a finite group, i.e., we study how to express these invariants in terms of a small number of them.

3.1. An especially simple case: If G is a reflection group

Let us recall the definition of a reflection group and Chevalley's theorem.

Definition 5. A matrix $A \in \mathrm{GL}_n(k)$ is called a *reflection* if and only if precisely one of its n eigenvalues is not equal to 1. A finite subgroup G of $\mathrm{GL}_n(k)$ is called a *reflection group* if and only if it is generated by reflections.

Remark 6. Being a reflection group is not a property of the abstract group underlying G but it depends on its faithful representation $G \subset \mathrm{GL}_n(k)$.

Theorem 7 (Chevalley [6]). *The invariant ring $k[X]^G$ of a finite matrix group $G \subset \mathrm{GL}_n(k)$ is generated by n algebraically independent homogeneous invariants if and only if G is a reflection group.*

Proof. See [6] for the "if" part, and [17, Theorem 2.4.1] for the converse. □

Corollary 8. *The invariant ring $k[X]^G$ of a finite permutation group $G \subset \mathfrak{S}_n$ is generated by n algebraically independent homogeneous invariants if and only if G is a product of symmetric groups $\mathfrak{S}_{n_1} \times \cdots \times \mathfrak{S}_{n_s}$ with $\sum_{j=1}^{s} n_j = n$ and each $\mathfrak{S}_{n_j}$ acting on the indeterminates $X_{n_1+\cdots+n_{j-1}+k}$, $1 \leq k \leq n_j$.*

Proof. For the "if" part, see Example 2 or [12]. For the "only-if" part, we have at first to notice that the matrix A_τ associated to a permutation $\tau \in \mathfrak{S}_n$ is always diagonalizable, and that its characteristic polynomial is $\prod_{j=1}^{r}(1 - z^{l_j})$ where $l(\tau) = (l_1, \ldots, l_r)$ is the cycle type (lengths of the cycles) of τ (it is easy to see from the block decomposition of A_τ associated to the cycle decomposition of τ). So, such a permutation τ acts as a reflection if and only if $l(\tau) = (1, \ldots, 1, 2)$, or in other words, if and only if τ is a

transposition. So, from Theorem 7, G must be generated by transpositions. But it is then easy to see that such a group must be a product of symmetric groups. □

Example 9. Here, we shall use the representation of the invariants of a reflection group G given by Chevalley's theorem to solve an algebraic system whose equations are invariant by the action of G. We apply here in fact the general algorithm of Section 5.1 to a particular case. The following system is quoted by K. Gatermann from [16]:

$$(\text{Noo})\begin{cases} P_1 = 1 - X_1(\alpha + X_2^2 + X_3^2) = 0, \\ P_2 = 1 - X_2(\alpha + X_3^2 + X_1^2) = 0, \\ P_3 = 1 - X_3(\alpha + X_1^2 + X_2^2) = 0, \end{cases}$$

where α is an independent parameter. The system (Noo) is equivalent to the following:

$$(\text{Noo}')\begin{cases} Q_1 = P_1 + P_2 + P_3 = 0, \\ Q_2 = P_1P_2 + P_2P_3 + P_3P_1 = 0, \\ Q_3 = P_1P_2P_3 = 0. \end{cases}$$

Each equation of this new system is invariant by the action of the symmetric group $\mathfrak{S}_3$, hence can be expressed in terms of $\Sigma_3 = X_1X_2X_3$, $\Sigma_2 = X_1X_2 + X_2X_3 + X_3X_1$ and $\Sigma_1 = X_1 + X_2 + X_3$: we get

$$Q_1 = 3\Sigma_3 - (\Sigma_2 + \alpha)\Sigma_1 + 3 = 0$$

which gives Σ_3 in terms of Σ_1 and Σ_2. We use this equation to eliminate Σ_3 in Q_2 and Q_3: we get respectively the polynomials $R_2(\Sigma_1, \Sigma_2)$ and $R_3(\Sigma_1, \Sigma_2)$. We then eliminate Σ_2 between R_2 and R_3 by computing a resultant; we get the following 3 families of solutions:

$$(\text{Noo1})\begin{cases} \Sigma_1 = 0, \\ \Sigma_2 = \alpha, \\ \Sigma_3 = -1, \end{cases} \qquad (\text{Noo2})\begin{cases} 0 = 2\Sigma_1^3 + 9\alpha\Sigma_1 - 27, \\ \Sigma_2 = (\tfrac{1}{3})\Sigma_1^2, \\ \Sigma_3 = (\tfrac{1}{2}) - (\alpha/6)\Sigma_1, \end{cases}$$

$$(\text{Noo3})\begin{cases} 0 = 2\alpha\Sigma_1^4 - 2\Sigma_1^3 + 9\alpha^2\Sigma_1^2 - 36\alpha\Sigma_1 + 4\alpha^3 + 27, \\ (98\alpha^3 - 54)\Sigma_2 = (42\alpha^3 - 18)\Sigma_1^2 + 93\alpha^2\Sigma_1 + 70\alpha^4 - 243\alpha, \\ \Sigma_3 = (\tfrac{1}{3})(\Sigma_2 + \alpha)\Sigma_1 - 1. \end{cases}$$

For each solution $(\sigma_1, \sigma_2, \sigma_3)$ of one of the systems (Noo1), (Noo2) or (Noo3), we get corresponding solutions (x_1, x_2, x_3) of (Noo): x_1, x_2 and x_3 are the 3 roots, sorted in any order, of the polynomial $T^3 - \sigma_1T^2 + \sigma_2T - \sigma_3$. And by this process, we get all the solutions of (Noo) (it follows from Theorem 23).

3.2. The Cohen–Macaulay algebra point of view

This point of view gives a very accurate description of polynomial invariants. It is in some way similar to the description of fractional invariants in Proposition 15. But

it involves usually more fundamental invariants than the description of Proposition 15 does, except for groups of index 2 ($[L : G] = 2$) which is the best case to apply this proposition to solve algebraic systems (see Remark 26).

Proposition 10. *Let G be a finite subgroup of $\mathrm{GL}_n(k)$. Then, $k[X]^G$ is a Cohen–Macaulay algebra over k, with Krull-dimension n. This means that we can find a family $(\Pi_1,\dots,\Pi_n)\in(k[X]^G)^n$ of homogeneous polynomials such that $k[X]^G$ be a finitely generated module over $k[\Pi_1,\dots,\Pi_n]$; and for any such choice $(\Pi_1,\dots,\Pi_n)$, $k[X]^G$ is a free module of dimension $(\prod_{i=1}^{e}\deg(\Pi_i))/|G|$ over $k[\Pi_1,\dots,\Pi_n]$.*

Proof. See [17, Theorems 2.3.1 and 2.3.5]. □

The polynomials Π_i are called *primary invariants* of G. A basis $(S_1,\dots,S_e)$ of $k[X]^G$ as a module over $k[\Pi_1,\dots,\Pi_n]$ is called a family of *secondary invariants* of G. Together, they make up a set of *fundamental invariants* of G. So, we can write

$$k[X]^G = \bigoplus_{i=1}^{e} k[\Pi_1,\dots,\Pi_n]S_i,$$

where the S_i are linearly independent over $k[\Pi_1,\dots,\Pi_n]$ and the Π_i are algebraically independent over k: this is the most accurate description of $k[X]^G$ we could dream of! According to [17], it is called the *Hironaka decomposition* of invariants. Algorithms are given in [17, 14] to find a system of fundamental invariants.

The following proposition will be helpful to link Proposition 10 to field theory. Therefore, it will enable us to apply the algorithm of field theory, based on linear algebra, to get the Hironaka decomposition of an invariant (see Proposition 12).

Proposition 11. *If $L\subset\mathrm{GL}_n(k)$ is a finite reflection group, then for any subgroup $G\subset L$, $k[X]^G$ is a free module over $k[X]^L$ of dimension $[L : G]$.*

Proof. The ring $k[X]^G$ is integral over $k[X]^L$ because every $P\in k[X]^G$ is a root of the monic polynomial $\prod_{Q\in LP}(T-Q)\in k[X]^L[T]$; and $k[X]^G$ is finitely generated as a $k[X]^L$-algebra. So, it is finitely generated as a $k[X]^L$-module. Now, from Theorem 7, $k[X]^L$ is generated by n algebraically independent homogeneous polynomials. Therefore, from Proposition 10, $k[X]^G$ is a free $k[X]^L$-module. Its dimension is of course that of $k(X)^G$ over $k(X)^L$, i.e., $[L : G]$ from Proposition 15. □

Consequently, applying Theorem 7, we can find a system of fundamental invariants $(\Pi_1,\dots,\Pi_n,S_1,\dots,S_e)$ of G, where $e = [L : G]$, such that $k[X]^L = k[\Pi_1,\dots,\Pi_n]$ and $k[X]^G = \bigoplus_{i=1}^{e} k[X]^L S_i$.

Proposition 12 (Effective Hironaka decomposition). *With the hypotheses of Proposition 11 and the previous notations, the coordinates $(A_1,\dots,A_e)\in(k[X]^L)^e$ of an $F\in k[X]^G$ in $(S_1,\dots,S_e)$ are the solutions of a linear Cramer system whose*

coefficients are the traces over $k[X]^L$ *(or "Reynolds projections") of the* S_iS_j *and* FS_i, $i,j \in \mathbb{N}_e^*$.

Proof. See after Proposition 19. □

Let us state two useful examples (notations of the example of Section 2.1).

Example 13. If $G \subset \mathfrak{S}_n$, then from Proposition 11 and Corollary 8 we can choose $\Pi_i = \Sigma_i$ for all $i \in \mathbb{N}_n^*$. Then, $k[X]^G$ is a free module over $k[X]^{\mathfrak{S}_n} = k[\Sigma]$ of dimension $e = [\mathfrak{S}_n : G]$.

Example 14. For the same reasons, if $G \subset \mathfrak{S}_{n_1} \times \cdots \times \mathfrak{S}_{n_s}$, then $k[X]^G$ is a free module over $k[X]^{\mathfrak{S}_{n_1} \times \cdots \times \mathfrak{S}_{n_s}} = k[\Sigma^{(1)}, \ldots, \Sigma^{(s)}]$ of dimension $\prod_{j=1}^{s} n_j!/|G|$.

3.3. The field theory point of view

The results (propositions and algorithms) of this section are extracted from the Galois theory article [7], where they are used, in the frame of permutation groups, to compute relative *Lagrange resolvents* (defined in [1] or [7]).

Proposition 15. *Let* L *and* G *be finite subgroups of* $\mathrm{GL}_n(k)$ *with* $G \subset L$, *and* $\Theta \in k(X)^G$ *a primitive invariant (see Definition* 1*) of* G *relatively to* L. *Then, we have* $k(X)^G = k(X)^L[\Theta]$, *and* $(1, \Theta, \ldots, \Theta^{e-1})$ *is a basis of* $k(X)^G$ *as a* $k(X)^L$*-vector space, where* $e = [L : G]$.

Proof. See [19, Lemma 1]. Other proof: $k(X) : k(X)^L$ is a Galois extension with Galois group L, because L acts faithfully and automorphically on $k(X)$. Now, we have $\mathrm{Gal}(k(X) : k(X)^L[\Theta]) = \mathrm{Stab}_L(\Theta) = G = \mathrm{Gal}(k(X) : k(X)^G)$. From Galois' duality theorem, we conclude that $k(X)^L[\Theta] = k(X)^G$. □

Such a primitive invariant Θ of G relative to L can be computed thanks to an algorithm due to K. Girstmair (see [11]), which yields an invariant of lowest possible degree. This algorithm was implemented by Ines Abdeljaoued in AXIOM (see [2]).

When $k(X)^L$ is a purely transcendental extension of k (i.e., when we can write $k(X)^L = k(\Pi_1, \ldots, \Pi_n)$, see Remark 18), we have the following analogy with Hironaka's decomposition of polynomial invariants:

$$k(X)^G = \bigoplus_{i=0}^{e-1} k(\Pi_1, \ldots, \Pi_n)\Theta^i.$$

Remark 16. It happens of course when L is a reflection group (from Theorem 7 and by taking the fraction fields of the rings), but not only, as proves the following proposition, where D_4 does not act like a reflection group (see Corollary 8).

Proposition 17. *We have* $k(X_1,X_2,X_3,X_4)^{D_4} = k(\Sigma_1,\Sigma_3,\Sigma_4,I)$, *where* D_4 *denotes the subgroup of* $\mathfrak{S}_4$ *generated by* (1 2) *and* (1 3 2 4) *and* $I = X_1X_2 + X_3X_4$.

Proof. From Proposition 15, $k(\boldsymbol{X})^{D_4} = k(\boldsymbol{X})^{\mathfrak{S}_4}(I) = k(\Sigma_1,\Sigma_2,\Sigma_3,\Sigma_4)(I)$. So, we just need to prove that $\Sigma_2 \in k(\Sigma_1,\Sigma_3,\Sigma_4,I)$. Indeed, computing the minimal polynomial of I over $k(\boldsymbol{X})^{\mathfrak{S}_4}$, we find $\Sigma_2 = I + (I\Sigma_1\Sigma_3 - \Sigma_3^2 - \Sigma_1^2\Sigma_4)/(I^2 - 4\Sigma_4)$. Another pure basis of $k(\boldsymbol{X})^{D_4}$ can also be found in [13, Section 2.4.2]. □

Beware. Yet, $k[\boldsymbol{X}]^{D_4}$ is not a module of finite type over the ring $R = k[\Sigma_1,\Sigma_3,\Sigma_4,I]$. Indeed, R is a polynomial ring (because from Proposition 17 and 3, the elements $\Sigma_1,\Sigma_3,\Sigma_4,I$ are algebraically independent over k). So, R is integrally closed. Now, Σ_2 does not belong to R, but we saw in Proposition 17 that it belongs to its fraction field $k(\Sigma_1,\Sigma_3,\Sigma_4,I)$. So, Σ_2 is not integral over R; hence $R[\Sigma_2]$ is not finitely generated as a module over R. Now, $R[\Sigma_2] \subset k[\boldsymbol{X}]^{D_4}$, and R is Noetherian, so that $k[\boldsymbol{X}]^{D_4}$ is not either finitely generated over R.

Remark 18. More generally, the problem of deciding whether the invariant field $k(\boldsymbol{X})^L$ of a finite group $L \subset \mathrm{GL}_n(k)$ is purely transcendental over k or not is known as *Noether's Problem*, and was addressed by Kemper in [13].

The following is an algorithmical version of Proposition 15.

Proposition 19. *The coordinates* $(A_0,\ldots,A_{e-1}) \in (k(\boldsymbol{X})^L)^e$ *of an* $F \in k(\boldsymbol{X})^G$ *in the basis* $(1,\Theta,\ldots,\Theta^{e-1})$ *over the field* $k(\boldsymbol{X})^L$, *with the hypothesis of Proposition* 15, *are the solutions of a linear Cramer system, whose coefficients belong to* $k[\boldsymbol{X}]^L$ *and are the traces over* $k(\boldsymbol{X})^L$ *of* $1,\Theta,\ldots,\Theta^{2e-2}$ *and* $P,P\Theta,\ldots,P\Theta^{e-1}$.

Proof. Let Tr denote the *trace function* on $k(\boldsymbol{X})^G$ over $k(\boldsymbol{X})^L$, i.e., the function defined by

$$\forall F \in k(\boldsymbol{X})^G, \qquad \mathrm{Tr}(F) = \frac{1}{|G|}\sum_{A\in L} A.F$$

(the application $[L:G]^{-1}\mathrm{Tr}$ is sometimes called the *Reynolds projection* from $k(\boldsymbol{X})^G$ onto $k(\boldsymbol{X})^L$).

We are looking for fractions $A_0,\ldots,A_{e-1} \in k(\boldsymbol{X})^L$ such that $F = \sum_{j=0}^{e-1} A_j\Theta^j$. Let us multiply this equation by Θ^i, for $i \in \mathbb{N}_{e-1}$, and apply the trace function; we get the following linear system:

$$(TS)\ \forall i \in \mathbb{N}_{e-1} \quad \mathrm{Tr}(F.\Theta^i) = \sum_{j=0}^{e-1} A_j \mathrm{Tr}(\Theta^{i+j}).$$

The extension $k(\boldsymbol{X})^G : k(\boldsymbol{X})^L$ is separable (as a subextension of the Galois extension $k(\boldsymbol{X}) : k(\boldsymbol{X})^L$); so, the trace bilinear $k(\boldsymbol{X})^L$-form $(F_1,F_2) \mapsto \mathrm{Tr}(F_1F_2)$ is not degenerated on $k(\boldsymbol{X})^G$ (see [5, A V.47 Proposition 1c]). Therefore, as $(1,\Theta,\ldots,\Theta^{e-1})$ is a

$k(\boldsymbol{X})^L$-basis of $k(\boldsymbol{X})^G$, the system (TS) is Cramer over the field $k(\boldsymbol{X})^L$, and we get the A_i by solving it. □

Proof of Proposition 12. We look for the family $(A_1,\dots,A_e)\in(k[\boldsymbol{X}]^L)^e$ such that $F=\sum_{j=1}^e A_jS_j$. Such polynomials A_i must satisfy: $\forall i\in\mathbb{N}_e^*$, $\mathrm{Tr}(FS_i)=\sum_{j=1}^e A_j\,\mathrm{Tr}(S_iS_j)$. This system is Cramer for the same reason as in Proposition 19 (we embed the algebras $k[\boldsymbol{X}]^G$ and $k[\boldsymbol{X}]^L$ in their fraction fields; $(S_1,\dots,S_e)$ is then a basis of $k(\boldsymbol{X})^G$ as a $k(\boldsymbol{X})^L$-vector space). Therefore, $(A_1,\dots,A_e)$ is the single solution of this system. □

Example 20. Examples 13 and 14 can obviously be transfered in terms of field theory. For instance, with $n=3$, $L=\mathfrak{S}_3$ and $\Theta=X_1+X_2$, we have $\mathrm{Stab}_L(\Theta)=G=\{\mathrm{Id},(1,2)\}$; so, from Proposition 15, $k(\boldsymbol{X})^G=k(\Sigma_1,\Sigma_2,\Sigma_3)[\Theta]$. Let us consider $F=X_1X_2$, which belongs to $k(\boldsymbol{X})^G$. Thanks to the algorithm of Proposition 19, we find $F=\Theta^2-\Sigma_1\Theta+\Sigma_2$.

Iterating the Propositions 15 and 19, we get the following propositions.

Proposition 21. *Let $(L=G_0,\dots,G_r=G)$ be a family of finite subgroups of $\mathrm{GL}_n(k)$ such that $L=G_0\supset G_1\supset\cdots\supset G_r=G$, and for all $i\in\mathbb{N}_r^*$, Θ_i an invariant of G_i relative to G_{i-1}. Then we have $k(\boldsymbol{X})^L[\Theta_1,\dots,\Theta_r]=k(\boldsymbol{X})^G$; and if we let $e_i=[G_{i-1}:G_i]$, then $(\prod_{j=1}^r\Theta_j^{i_j})_{1\le i_j\le e_j,\forall j\in\mathbb{N}_r^*}$ is a basis of $k(\boldsymbol{X})^G$ as a vector space over $k(\boldsymbol{X})^L$. Its dimension is $e=[L:G]=\prod_{j=1}^r e_j$.*

Proposition 22. *With the hypothesis of Proposition 21, we have an algorithm, based on linear algebra, to compute the coordinates of an $F\in k(\boldsymbol{X})^G$ in the $k(\boldsymbol{X})^L$-basis $(\prod_{j=1}^r\Theta_j^{i_j})_{1\le i_j\le e_j,\forall j\in\mathbb{N}_r^*}$.*

Proof. We iterate r times the algorithm of Proposition 19. More accurately, at the level r, if we look for the decomposition $F=\sum_{j=0}^{e_r-1}A_j\Theta_r^j$ of an $F\in k(\boldsymbol{X})^G$, with $A_j\in k(\boldsymbol{X})^L[\Theta_1,\dots,\Theta_{r-1}]$, we just need to write the linear system

$$\forall i\in\mathbb{N}_{e_r-1}\quad \mathrm{Tr}_{r/r-1}(F.\Theta_r^i)=\sum_{j=0}^{e_r-1}A_j\mathrm{Tr}_{r/r-1}(\Theta_r^{i+j})$$

where $\mathrm{Tr}_{r/r-1}$ denotes the trace function on $k(\boldsymbol{X})^{G_r}$ over $k(\boldsymbol{X})^{G_{r-1}}$, and before solving this system, to use the algorithm at level $r-1$ to express its coefficients $\mathrm{Tr}_{r/r-1}(\Theta_r^{i+j})$ (with $0<i+j\le e$; it's enough because the coefficients $\mathrm{Tr}_{r/r-1}(\Theta^k)$ with $e<k\le 2e-2$ can be deduced from the $\mathrm{Tr}_{r/r-1}(\Theta^k)$ with $1\le k\le e$ thanks to Newton's formulae) and $\mathrm{Tr}_{r/r-1}(F.\Theta_r^i)$ as a polynomial in $\Theta_1,\dots,\Theta_{r-1}$ with coefficients in $k(\boldsymbol{X})^L$. By induction, we are reduced to $r=1$, in which case we apply Proposition 19.

4. Solving algebraic systems with symmetries

Let us consider the system (F) defined in Section 2.2. As mentioned in that section, the equations $F_i=0$ in (F) satisfy $A.F_i=F_i$ for every $A\in G$. Let L be a subgroup of $\mathrm{GL}_n(k)$ such that $G\subset L$ and that $k(\boldsymbol{X})^L$ be a purely transcendental extension of k, $\Pi_1,\ldots,\Pi_n$ polynomials such that $k(\boldsymbol{X})^L=k(\Pi_1,\ldots,\Pi_n)$, and $\Theta\in k[\boldsymbol{X}]^G$ a primitive polynomial invariant of G relatively to L. When it is possible, it is convenient to choose Θ among the polynomials F_i of the system.

Then thanks to the algorithm of Proposition 19, we can express each polynomial F_i as an algebraic fraction in $\Pi_1,\ldots,\Pi_n$ and Θ, polynomial in Θ:

$$\forall i\in\mathbb{N}_p^* \quad F_i(\boldsymbol{X})=H_i(\Pi_1,\ldots,\Pi_n,\Theta).$$

Now, let L be the minimal polynomial of Θ over $k[\boldsymbol{X}]^L$; we have

$$L(\boldsymbol{X},T)=\prod_{\Theta'\in L.\Theta}(T-\Theta')\in k[\boldsymbol{X}]^L[T]$$

(see [1] or [7], where L is called a *generic Lagrange resolvent*).

As $k(\Pi_1,\ldots,\Pi_n)=k(\boldsymbol{X})^L$, we can write

$$L(\boldsymbol{X},T)=H_0(\Pi_1,\ldots,\Pi_n,T)$$

where H_0 is some rational fraction. The equation $H_0(\Pi_1,\ldots,\Pi_n,\Theta)=0$ is always satisfied because Θ is a root of L. Then, we solve the system of $(p+1)$ algebraic equations $\forall i\in\mathbb{N}_p, H_i(\Pi_1,\ldots,\Pi_n,\Theta)=0$, in $\Pi_1,\ldots,\Pi_n,\Theta$ seen as indeterminates.

The following theorem is then obvious:

Theorem 23. *Let $D\in k[\Pi_1,\ldots,\Pi_n]$ be the LCM of the denominators of all the fractions H_i, $i\in\mathbb{N}_p$, and let $H_i'=DH_i$. For every solution $(x_1,\ldots,x_n)$ of the system $(F):\forall i\in\mathbb{N}_p^*, F_i(\boldsymbol{X})=0$, there exists a solution $(\pi_1,\ldots,\pi_n,\theta)$ of the system $(H'):\forall i\in\mathbb{N}_p, H_i'(\Pi_1,\ldots,\Pi_n,\Theta)=0$ such that $(x_1,\ldots,x_n)$ is a solution of the system $(P_\pi):\forall i\in\mathbb{N}_n^*, \Pi_i(\boldsymbol{X})=\pi_i$ and of the equation $\Theta(\boldsymbol{X})=\theta$. Conversely, for any solution $(\pi_1,\ldots,\pi_n,\theta)$ of the system (H') such that $D(\pi_1,\ldots,\pi_n)\neq 0$, if $\boldsymbol{x}=(x_1,\ldots,x_n)$ is a solution of the system (P_π) relative to $(\pi_1,\ldots,\pi_n)$, then there exists some $A\in L$ such that $\Theta(A.\boldsymbol{x})=\theta$, and then for all $B\in G$, $BA.\boldsymbol{x}$ is a solution of the system (F).*

Proof. If $\boldsymbol{x}=(x_1,\ldots,x_n)$ is a solution of F, then let $\pi_i=\Pi_i(\boldsymbol{x})$ for all $i\in\mathbb{N}_n^*$ and $\theta=\Theta(\boldsymbol{x})$. For all $i\in\mathbb{N}_n^*$, $F_i(\boldsymbol{x})=0$ implies: $D(\pi_1,\ldots,\pi_n)F_i(\boldsymbol{x})=0$, and as $D(\Pi_1(\boldsymbol{X}),\ldots,\Pi_n(\boldsymbol{X}))F_i(\boldsymbol{X})=H_i'(\Pi_1,\ldots,\Pi_n,\Theta)$ in $k[\boldsymbol{X}]$, we have $H'(\pi_1,\ldots,\pi_n,\theta)=0$. And for $i=0$, $H_0(\pi_1,\ldots,\pi_n,\theta)=L(\boldsymbol{x},\theta)=\prod_{\Theta'\in L.\Theta}(\theta-\Theta'(\boldsymbol{x}))=0$. So, $\boldsymbol{x}$ is solution of (P_π) and $(\pi_1,\ldots,\pi_n,\theta)$ is a solution of (H').

Conversely, if $(\pi_1,\ldots,\pi_n,\theta)$ is a solution of (H') and $\boldsymbol{x}$ is a solution of (P_π), then

$$\prod_{\Theta'\in L.\Theta}(\theta-\Theta'(\boldsymbol{x}))=L(\boldsymbol{x},\theta)=H_0(\pi_1,\ldots,\pi_n,\theta)=0.$$

So, there exists $\Theta' \in L.\Theta$ such that $\Theta'(\boldsymbol{x})=\theta$. There exists $A \in L$ such that $\Theta'=A^{-1}.\Theta$; then, $\Theta(A.\boldsymbol{x})=\theta$. Now, for all $i \in \mathbb{N}_p^*$ and for all $B \in G$, we have $D(\pi_1,\ldots,\pi_n)F_i(BA.\boldsymbol{x}) = D(\pi_1,\ldots,\pi_n)H_i(\pi_1,\ldots,\pi_n,\theta)=H_i'(\pi_1,\ldots,\pi_n,\theta)=0$; so if we assume that $D(\pi_1,\ldots,\pi_n)\neq 0$, then $F_i(BA.\boldsymbol{x})=0$. □

Remark 24. If we choose for Θ one of the F_i, then we can substitute $\Theta=0$ in the H_i and get a system in the indeterminates $\Pi_1,\ldots,\Pi_n$. Then, the polynomial $H_0(\Pi_1,\ldots,\Pi_n,0)$ is reduced to $\prod_{\Theta' \in L.\Theta} \Theta' \in k[\boldsymbol{X}]^L$, i.e., the norm of Θ over $k(\boldsymbol{X})^L$, in terms of $\Pi_1,\ldots,\Pi_n$.

Using Proposition 21 instead of Proposition 15, Theorem 23 is based on Proposition 15, where we use a primitive element of $k(\boldsymbol{X})^G : k(\boldsymbol{X})^L$. We can break this extension of fields, as in Proposition 21, whose notations we keep, and modify consequently Theorem 23.

So, we define fractions F_i that are polynomial in $\Theta_1,\ldots,\Theta_r$ such that

$$\forall i \in \mathbb{N}_p^* \quad F_i(\boldsymbol{X})=H_i(\Pi_1,\ldots,\Pi_n,\Theta_1,\ldots,\Theta_r).$$

We define, for all $j \in \mathbb{N}_r^*$, the polynomial $L_j(\boldsymbol{X},T)=\prod_{\Theta' \in G_{j-1}.\Theta_j}(T-\Theta')$. It belongs to $k[\boldsymbol{X}]^{G_{j-1}}[T] \subset k(\Pi_1,\ldots,\Pi_n)[\Theta_1,\ldots,\Theta_{j-1}][T]$. Let N_j be defined by: $L_j(\boldsymbol{X},T)=N_j(\Pi_1,\ldots,\Pi_n,\Theta_1,\ldots,\Theta_{j-1},T)$, polynomial in $\Theta_1,\ldots,\Theta_r,T$ and fractional in the Π_i. Then, we get the following variant of Theorem 23:

Theorem 25. *Let $D \in k[\Pi_1,\ldots,\Pi_n]$ be the LCM of the denominators of all the fractions H_i, $i \in \mathbb{N}_p^*$, and N_j, $j \in \mathbb{N}_r^*$. Let $H_i'=DH_i$ for all i and $N_j'=DN_j$ for all j. For every solution $\boldsymbol{x}=(x_1,\ldots,x_n)$ of the system $(F):(\forall i \in \mathbb{N}_p^*, F_i(\boldsymbol{X})=0)$, there exists a solution $(\pi_1,\ldots,\pi_n,\theta_1,\ldots,\theta_r)$ of the system $(H',N'):(\forall i \in \mathbb{N}_p^*, H_i'(\Pi_1,\ldots,\Pi_n,\Theta_1,\ldots,\Theta_r)=0$ and $\forall j \in \mathbb{N}_r^*, N_j(\Pi_1,\ldots,\Pi_n,\Theta_1,\ldots,\Theta_j)=0)$ such that $\boldsymbol{X}$ be a solution of the system $(P_\pi):\forall i \in \mathbb{N}_n^*, \Pi_i(\boldsymbol{X})=\pi_i$ and of the equations $\Theta_1(\boldsymbol{X})=\theta_1,\ldots,\Theta_r(\boldsymbol{X})=\theta_r$. Conversely, for any solution $(\pi_1,\ldots,\pi_n,\theta_1,\ldots,\theta_r)$ of the system (H',N') such that $D(\pi_1,\ldots,\pi_n)\neq 0$, if $\boldsymbol{x}$ is a solution of the system (P_π) relative to $(\pi_1,\ldots,\pi_n)$, then there exists $A \in \mathrm{GL}_n(k)$ such that $\forall j \in \mathbb{N}_r^*, \Theta_j(A.\boldsymbol{x})=\theta_j$, and then for every $B \in G$, $BA.\boldsymbol{x}$ is a solution of the system (F).*

Proof. It is roughly the same as that of Theorem 23. □

5. Examples

5.1. Sum-up of the method

Here, we recall the different steps of the general algorithm, either by using the Cohen–Macaulay algebra point of view (denoted *infra* by (CMA)) or by using field

theory (denoted *infra* by (FT)). With the aim to simplify, we consider here Theorem 23, not Theorem 25 (see in Section 5.4 an example with Theorem 25).

Input: A system (F): $\forall i \in \mathbb{N}_p^*$, $F_i(X_1,\ldots,X_n)=0$, and a finite subgroup G of $\mathrm{GL}_n(k)$ such that $\forall i \in \mathbb{N}_p^*$, $F_i \in k[\boldsymbol{X}]^G$.

Successive steps:

(i) Find, if possible, a finite subgroup L of $\mathrm{GL}_n(k)$ such that $G \subset L$ and that either L be a reflection group (case (CMA), see Definition 5) either L satisfy Noether's problem, (case (FT), see Remark 18).

(ii) Compute a pure transcendent basis $(\Pi_1,\ldots,\Pi_n)$ of $k[\boldsymbol{X}]^L$ (case (CMA)) or of $k(\boldsymbol{X})^L$ (case (FT)), and then the whole Hironaka decomposition $\bigoplus_{i=1}^{e} k[\Pi_1,\ldots,\Pi_n]S_i$ of $k[\boldsymbol{X}]^G$ (case (CMA), see the algorithms in Section 3.2) or $\bigoplus_{i=0}^{e-1} k(\Pi_1,\ldots,\Pi_n)\Theta^i$ of $k(\boldsymbol{X})^G$ (case (FT), see Section 3.3).

(iii) Express the polynomials F_i, $1 \le i \le p$, in terms of the fundamental invariants thanks to Proposition 12 (Case (CMA)) or 19 (case (FT)).

(iv) In the case (CMA), we assume that $e \le 2$ and $S_1 = 1$. We are then reduced to the case (FT), by letting $\Theta = S_2$ if $e=2$. In both cases (CMA) or (FT), compute the minimal polynomial of Θ over $k[\boldsymbol{X}]^L$, and then solve the system (H') (see Theorem 23) in the variables $\Pi_1,\ldots,\Pi_n,\Theta$.

Remark 26. In the case (CMA) with $e>2$, we should add to the system (H') the generators of the ideal of the syzygies between the secondary invariants. We shall not deal with this case in this article.

(v) For each solution $(\pi_1,\ldots,\pi_n,\theta)$ of (H'), solve the corresponding system (P_π): $\forall i \in \mathbb{N}_n^*, \Pi_i(\boldsymbol{X})=\pi_i$, and in each orbit of L in the set of the solutions of (P_π), keep one solution $\boldsymbol{x}=(x_1,\ldots,x_n)$ such that $\Theta(\boldsymbol{x})=\theta$ (it costs at most $[L:G]$ tries for each orbit). Let S be the set of all these solutions $\boldsymbol{x}$.

Remark 27. Solving (P_π) when L is a product of symmetric groups is particularly easy. For instance, when $L=\mathfrak{S}_n$, we can choose $\Pi_i=\Sigma_i$ for every $i \in \mathbb{N}_n^*$, so that the solutions of (P_π) are exactly the families of roots, taken in some order, of the polynomial $T^n + \sum_{i=1}^{n}(-1)^i \pi_i T^{n-i}$.

(vi) For every $\boldsymbol{x}$ in S, check whether D cancels on $\boldsymbol{x}$. If it does not, we can keep $\boldsymbol{x}$; if it does, we have to check that $\boldsymbol{x}$ satisfies (F), and we throw it if it does not. Let S' be the set of all the $\boldsymbol{x}$ we have kept.

Output: The set of all solutions of (F) is $\{A.\boldsymbol{x} / A \in G,\ \boldsymbol{x} \in S'\}$.

Implementation: The algorithm is implemented in the AXIOM computer algebra language (see [2]), when $L=\mathfrak{S}_n$ and the principal invariants are the elementary symmetric polynomials $\Sigma_1,\ldots,\Sigma_n$. We implemented a domain that computes on symmetric

polynomials, represented either as polynomials in the Σ_i, or as linear combinations of the polynomials $M_i = \sum_{\tau \in \mathfrak{S}_n} \prod_{j=1}^{n} X_j^{i_{\tau(j)}}$. Then, we implemented the algorithms of Propositions 19 and 22. Besides, computation in $k[\boldsymbol{X}]^{\mathfrak{S}_{n_1} \times \cdots \times \mathfrak{S}_{n_s}}$ is implemented in SYM (see [18]), with many operations on symmetric polynomials.

5.2. *With a group of matrices, using the CMA point of view*

Let us consider the following system:

$$(\text{Rot}) \begin{cases} P_1 = X_1^4 + X_2^4 - 1 = 0, \\ P_2 = X_1^3 X_2^3 (X_1^6 - X_2^6) - 2 = 0. \end{cases}$$

If we try to eliminate X_2 between the two equations thanks to a resultant, we get a horrible irreducible polynomial in X_1 of degree 48, which depends only on X_1^4; so, we have to find the roots of an irreducible polynomial of degree 12 and then to extract their fourth roots. Using the symmetries, we will show that we are reduced to a polynomial of degree 6 and extracting fourth roots.

Each equation of the system is invariant by the matrix

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

hence by the action of the cyclic group $G = \{\text{Id}, A, -\text{Id}, -A\}$ generated by A. We compute the following family of primary invariants of G: $\Pi_1 = X_1^2 + X_2^2$ and $\Pi_2 = (X_1 X_2)^2$, and the corresponding single secondary invariant $S = X_1 X_2 (X_1^2 - X_2^2)$ (they are given in [17, Example 2.2.4]), so that $k[\boldsymbol{X}]^G = k[\Pi_1, \Pi_2] \oplus k[\Pi_1, \Pi_2] S$. Then, we express the system in terms of the fundamental invariants, thanks to the algorithm of Proposition 19. We get: $P_1 = \Pi_1^2 - 2\Pi_2 - 1$ and $P_2 = (\Pi_1^2 \Pi_2 - \Pi_2^2) S - 2$. Besides, we compute $S^2 - \Pi_1^2 \Pi_2 + 4\Pi_2^2 = 0$ (minimal polynomial of S over $k[\Pi_1, \Pi_2]$). So, (Rot) is equivalent to

$$(\text{Rot}') \begin{cases} (\Pi_1^2 - \Pi_2) S \Pi_2 - 2 = 0, \\ \Pi_1^2 - 2\Pi_2 - 1 = 0, \\ S^2 - \Pi_1^2 \Pi_2 + 4\Pi_2^2 = 0, \\ S - X_1 X_2 (X_1^2 - X_2^2) = 0. \end{cases}$$

We eliminate Π_1 in the first and the third equations thanks to the second one, and then we eliminate Π_2, getting

$$S^6 + 3S^4 + 8S^3 - 6S + 16 = 0.$$

For each solution s of this equation of degree 6, we compute the values π_1 and π_2 of Π_1 and Π_2 s.t. (s, π_1, π_2) satisfy (Rot′). Then, the solutions (x_1, x_2) of (Rot) must satisfy $(x_1^2 - x_2^2)^2 = s^2/\pi_2$. So, we know $x_1^2 - x_2^2$ up to the sign and $x_1^2 + x_2^2 = \pi_1$, from which we deduce all the solutions (x_1, x_2) of (Rot).

So, we have reduced the problem from degree 12 to degree 6.

5.3. Using (FT) with a simple extension of $k(\Sigma)$

Cyclic roots systems come from the problem of finding bi-equimodular vectors (see [3,4], where these systems are solved for $n=4,5,6,7$). In this paragraph, we apply Theorem 23 to the following 5th-cyclic roots system, with $L=\mathfrak{S}_5$, $\Pi_i=\Sigma_i, \forall i\in\mathbb{N}_5^*$, and $G=D_5=\langle(1\,2\,3\,4\,5),(2\,5)(3\,4)\rangle$:

$$(S_5):\quad \begin{cases} X_1+X_2+X_3+X_4+X_5=0,\\ X_1X_2+X_2X_3+X_3X_4+X_4X_5+X_5X_1=0,\\ X_1X_2X_3+X_2X_3X_4+X_3X_4X_5+X_4X_5X_1+X_5X_1X_2=0,\\ X_1X_2X_3X_4+X_2X_3X_4X_5+X_3X_4X_5X_1+X_4X_5X_1X_2+X_5X_1X_2X_3=0,\\ X_1X_2X_3X_4X_5-1=0. \end{cases}$$

Let $\Theta=X_1X_2+X_2X_3+X_3X_4+X_4X_5+X_5X_1$. Then (S_5) is equivalent to

$$(S_5'):\quad (\Sigma_1=0,\Theta=0,P=0,\Sigma_4=0,\Sigma_5-1=0),$$

where $P=X_1X_2X_3+X_2X_3X_4+X_3X_4X_5+X_4X_5X_1+X_5X_1X_2$.

Let us use Remark 24: as $\Theta=0$ is one of the equations of (S_5), we can compute, instead of the polynomial L, the norm $C(\Sigma_1,\dots,\Sigma_5)$ of Θ over $k(\Sigma)$, i.e., the product of the 12 elements of $\mathfrak{S}_5.\Theta$.

Now, thanks to the algorithm of Section 3.3, we find the polynomials A_i and B_i with $\gcd(A_i,B_i)=1$, $0\le i\le 11$, such that

$$P=\sum_{i=0}^{11}\frac{A_i(\Sigma_1,\Sigma_2,\Sigma_3,\Sigma_4,\Sigma_5)}{B_i(\Sigma_1,\Sigma_2,\Sigma_3,\Sigma_4,\Sigma_5)}\Theta^i.$$

Let $D(\Sigma)=\prod_{i=0}^{11}B_i(\Sigma)$. Replacing Σ_1 and Σ_4 by 0 and Σ_5 by 1, we get $\bar{A}_0(\Sigma_2,\Sigma_3)=A_0(0,\Sigma_2,\Sigma_3,0,1)$, $\bar{B}_0(\Sigma_2,\Sigma_3)=B_0(0,\Sigma_2,\Sigma_3,0,1)$, $\bar{C}(\Sigma_2,\Sigma_3)=C(0,\Sigma_2,\Sigma_3,0,1)$ and $\bar{D}(\Sigma_2,\Sigma_3)=D(0,\Sigma_2,\Sigma_3,0,1)$. We compute

$$\begin{aligned}\bar{A}_0&=2\Sigma_2^2\Sigma_3^7+89\Sigma_2\Sigma_3^6+125\Sigma_3^5+41\Sigma_2^4\Sigma_3^4+550\Sigma_2^3\Sigma_3^3-5^5\Sigma_2^2\Sigma_3^2\\&\quad+(189\Sigma_2^6-6250\Sigma_2)\Sigma_3-1125\Sigma_2^5,\\ \bar{B}_0&=2\Sigma_2^2\Sigma_3^6+58\Sigma_2\Sigma_3^5+31\Sigma_2^4\Sigma_3^3+325\Sigma_2^3\Sigma_3^2-625\Sigma_2^2\Sigma_3+108\Sigma_2^6+5^5\Sigma_2,\\ \bar{C}&=-27\Sigma_2^7-4\Sigma_3^3\Sigma_2^5-150\Sigma_3^2\Sigma_2^4+(-12\Sigma_3^5+5^5)\Sigma_2^2-125\Sigma_3^4\Sigma_2+\Sigma_3^8,\end{aligned}$$

$$\mathrm{Res}_{\Sigma_3}(\bar{A}_0,\bar{C})=-\Sigma_2^{10}(\Sigma_2^5+5^5)^6(24(6\Sigma_2)^5-5^5)(27\Sigma_2^{10}+7974\Sigma_2^5-5^5)^2.$$

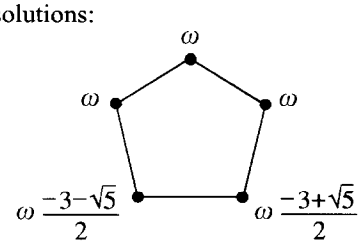
From Theorem 23, we know that a necessary condition satisfied by a solution x of (S_5) is that $\bar{A}_0\bar{D}(\sigma_2,\sigma_3)=\bar{C}(\sigma_2,\sigma_3)=0$, where $\sigma_2=\Sigma_2(x)$ and $\sigma_3=\Sigma_3(x)$, which implies that σ_2 be a root of $\mathrm{Res}_{\Sigma_3}(\bar{A}_0\bar{D},\bar{C})=\mathrm{Res}_{\Sigma_3}(\bar{A}_0,\bar{C})\mathrm{Res}_{\Sigma_3}(\bar{D},\bar{C})$. Now, this condition is not sufficient, because the solutions cancel the denominator D, as shows the following

resultant:

$$\mathrm{Res}_{\Sigma_3}(\bar{B}_0, \bar{C}) = -\Sigma_2^8(\Sigma_2^5 + 5^5)^5(24(6\Sigma_2)^5 - 5^5)(27\Sigma_2^{10} + 7974\Sigma_2^5 - 5^5)^2.$$

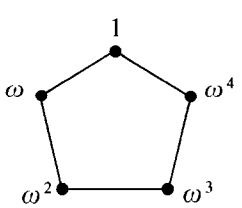
In fact, the roots of $\mathrm{Res}_{\Sigma_3}(\bar{D}, \bar{C})$ give no solution of (S_5') that be not already a solution coming from $\mathrm{Res}_{\Sigma_3}(\bar{A}_0, \bar{C})$; and in $\mathrm{Res}_{\Sigma_3}(\bar{A}_0, \bar{C})$, the only factors that lead to solutions of (S_5) are Σ_2 and $\Sigma_2^5 + 5^5$: we could prove this by an argument of multiplicity (see a forthcoming paper), but we can also simply verify it by computing all those candidate solutions and see that they do not satisfy (S_5). So, the only solutions are given by $\Sigma_2 = 0$ or $\Sigma_2^5 = (-5)^5$.

Case 1: $\Sigma_2^5 = (-5)^5$. The solutions for Σ_2 are: $\sigma_2 = -5\omega^2$, where ω is a fifth root of unity. To each solution σ_2 for Σ_2 corresponds a single solution for Σ_3: $\sigma_3 = -5\omega^3$; and we know that the only values for $\Sigma_1, \Sigma_4, \Sigma_5$ are $\sigma_1 = 0$, $\sigma_4 = 0$ and $\sigma_5 = 1$. The corresponding values x_i for the X_i are the solutions of the system: $\Sigma_i(X_1, X_2, X_3, X_4, X_5) = \sigma_i$, for $i = 1, 2, 3, 4, 5$ (which are of course the roots of the polynomial $T^5 - 5\omega^2 T^3 + 5\omega^3 T^2 - 1$), i.e., ω, ω, ω, $\omega(-3 - \sqrt{5})/2$, $\omega(-3 + \sqrt{5})/2$, ordered so that $\Theta(x_1, x_2, x_3, x_4, x_5) = 0$. For each of the 5 values of ω, 10 different orders are allowed. It leads to the following 50 solutions:



where ω is one of the five fifth roots of unity, and the vertices of the pentagon denote the roots, in the order x_1, x_2, x_3, x_4, x_5, beginning with any vertex and going along either clockwise or anticlockwise.

Case 2: $\Sigma_2 = 0$. If we replace Σ_2 by $\sigma_2 = 0$ in $C(\Sigma_2, \Sigma_3)$, we get $\Sigma_3 = 0$. The corresponding values x_i for the X_i are the roots of $T^5 - 1$, i.e., the fifth roots of unity, ordered so that $\Theta(x_1, x_2, x_3, x_4, x_5) = 0$; we get the following 20 solutions:



where ω is either $e^{2i\pi/5}$ or $e^{4i\pi/5}$ (the values $e^{8i\pi/5}$ and $e^{6i\pi/5}$ of ω would lead to the same solutions up to a symmetry).

Hence, (S_5) has exactly the $50 + 20 = 70$ solutions written above.

5.4. Breaking the simple extension of $k(\Sigma)$

Here, we look for an improvement of the method of Section 5.3, the notation of which we keep: we study the same system (S_5), but we use Theorem 25 instead of Theorem 23.

We notice that the alternating group $G_1 = A_5 = \langle (1\,2\,3), (1\,2\,4), (1\,2\,5)\rangle$ satisfies

$$G \subset G_1 \subset G_0 = \mathfrak{S}_5.$$

From Proposition 21, to this group corresponds the following field extension:

$$k(X)^{\mathfrak{S}_5} = k(\Sigma) \subset k(X)^{A_5} = k(\Sigma)[V] \subset k(X)^{G} = k(\Sigma)[\Theta] = k(\Sigma)[V][\Theta],$$

where V is the following (primitive) invariant of A_5: $V = \prod_{i<j}(X_j - X_i)$.

Then we do as in Section 5.3; the only difference is the way we express P. Here, we use the algorithm of Proposition 22 to express P as

$$P = \sum_{i=0}^{5} \frac{A_i(\Sigma_1,\Sigma_2,\Sigma_3,\Sigma_4,\Sigma_5)V + A_i'(\Sigma_1,\Sigma_2,\Sigma_3,\Sigma_4,\Sigma_5)}{B_i(\Sigma_1,\Sigma_2,\Sigma_3,\Sigma_4,\Sigma_5)}\Theta^i,$$

where the A_i, A_i' and B_i are polynomials. Let $\bar{A}_0(\Sigma_2,\Sigma_3)$, $\bar{A}_0'(\Sigma_2,\Sigma_3)$ and $\bar{B}_0(\Sigma_2,\Sigma_3)$ be the evaluations of respectively A_0, A_0' and B_0 on $(0,\Sigma_2,\Sigma_3,0,1)$. We compute

$$\begin{aligned}
\bar{A}_0 &= 210\Sigma_2\Sigma_3^7 + 6000\Sigma_3^6 + 30\Sigma_2^4\Sigma_3^5 + 2375\Sigma_2^3\Sigma_3^4 + 25\,000\Sigma_2^2\Sigma_3^3 \\
&\quad + (270\Sigma_2^6 + 250\,000\Sigma_2)\Sigma_3^2 + (-1125\Sigma_2^5 - 390\,625)\Sigma_3 + 140\,625\Sigma_2^4 \\
\bar{A}_0' &= 216\Sigma_3^{11} + 86\Sigma_2^3\Sigma_3^9 + 7590\Sigma_2^2\Sigma_3^8 + (8\Sigma_2^6 - 48\,000\Sigma_2)\Sigma_3^7 \\
&\quad + (1990\Sigma_2^5 + 175\,000)\Sigma_3^6 + 42\,075\Sigma_2^4\Sigma_3^5 + (144\Sigma_2^8 - 71\,875\Sigma_2^3)\Sigma_3^4 \\
&\quad + (8730\Sigma_2^7 - 3\,531\,250\Sigma_2^2)\Sigma_3^3 + (138\,375\Sigma_2^6 + 12\,890\,625\Sigma_2)\Sigma_3^2 \\
&\quad + (486\Sigma_2^{10} - 1\,406\,250\Sigma_2^5 - 9\,765\,625)\Sigma_3 + 12\,150\Sigma_2^9 + 703\,125\Sigma_2^4 \\
\bar{B}_0 &= 1458\Sigma_2^{10} + 216\Sigma_3^3\Sigma_2^8 + 24\,300\Sigma_3^2\Sigma_2^7 + 8\Sigma_3^6\Sigma_2^6 + (3168\Sigma_3^5 + 1\,856\,250)\Sigma_2^5 \\
&\quad + 120\,000\Sigma_3^4\Sigma_2^4 + (118\Sigma_3^8 + 450\,000\Sigma_3^3)\Sigma_2^3 + (11\,400\Sigma_3^7 + 3\,750\,000\Sigma_3^2)\Sigma_2^2 \\
&\quad + 187\,500\Sigma_3^6\Sigma_2 + 432\Sigma_3^{10} + 350\,000\Sigma_3^5 - 19\,531\,250.
\end{aligned}$$

Now, we apply Theorem 25. We compute (notations of Theorem 25) the polynomials $N_1(\Sigma, V)$ and $N_2(\Sigma, V, \Theta)$. Let C_1 and C_2 denote the residues of these polynomials modulo $(\Sigma_1 = 0,\ \Sigma_4 = 0,\ \Sigma_5 = 1,\ \Theta = 0)$. We find

$$\begin{aligned}
C_1 &= V^2 - 108\Sigma_3^5 - 16\Sigma_2^3\Sigma_3^3 - 825\Sigma_2^2\Sigma_3^2 + 3750\Sigma_2\Sigma_3 - 108\Sigma_2^5 - 3125, \\
C_2 &= \Sigma_2 V - 2\Sigma_3^4 - 15\Sigma_2^2\Sigma_3 + 125\Sigma_2.
\end{aligned}$$

Then, we compute

$$\mathrm{Res}_{\Sigma_3}(\mathrm{Res}_V(\bar{A}_0V+\bar{A'}_0,C_2),\mathrm{Res}_V(C_1,C_2))=\Sigma_2^{10}(\Sigma_2^5+5^5)^7 f_1f_2^2f_3f_4,$$

$$\mathrm{Res}_{\Sigma_3}(\bar{B}_0,\mathrm{Res}_V(C_1,C_2))=(\Sigma_2^5+5^5)^6 f_1f_2^2f_3f_4,$$

where

$$f_1=27\Sigma_2^5-1,$$

$$f_2=27\Sigma_2^{10}+7974\Sigma_2^5-3125,$$

$$f_3=256\Sigma_2^{15}+21\,089\,952\Sigma_2^{10}+1\,587\,890\,625\Sigma_2^5+30\,517\,578\,125$$

$$f_4=5\,038\,848\Sigma_2^{20}+1\,941\,472\,800\,000\Sigma_2^{15}+81\,696\,996\,562\,500\,000\Sigma_2^{10}$$
$$+910\,077\,209\,472\,656\,250\,000\Sigma_2^5-298\,023\,223\,876\,953\,125.$$

We conclude like in Section 5.3: $\Sigma_2=0$ or $\Sigma_2^5=(-5)^5$.

Beware. The polynomial C_2 in Section 5.4 is the norm of Θ over $k(\boldsymbol{X})^{\mathfrak{A}_5}$, whereas in Section 5.3 we used the norm C of Θ over $k(\boldsymbol{X})^{\mathfrak{S}_5}$. If we had used here the norm over $k(\boldsymbol{X})^{\mathfrak{S}_5}$, a big irreducible parasite factor of degree 60 would have appeared in the resultant $\mathrm{Res}_{\Sigma_3}(\mathrm{Res}_V(\bar{A}_0V+\bar{A}'_0,C_1),C)$. Indeed, the polynomials $\Sigma_1,\ldots,\Sigma_5,V,\Theta$ are not algebraically independent; if we want to lift the solutions in $\Sigma_1,\ldots,\Sigma_5,V,\Theta$ back to solutions in $X_1,\ldots,X_n$, we need to check that they satisfy the algebraic relations between these polynomials. It is sufficient that they satisfy (C_1 and C_2), but (C_1 and C) is not enough. This is implicit in Theorem 25. I would like to thank Marc Giusti here for pointing out to me this difficulty.

5.5. *Using (CMA) with a simple extension of* $k(\boldsymbol{X})^{\mathfrak{S}_{n_1}\times\cdots\times\mathfrak{S}_{n_s}}$

In this example, the system is dehomogenized, which destroys some of its symmetries but yet simplifies its resolution. This idea and a computation on (S_5) which inspired the following one are due to Daniel Lazard [15], whom I would like to thank here for his help.

Here, we solve the following system (S_6):

$$X_1+X_2+X_3+X_4+X_5+X_6=0,$$
$$X_1X_2+X_2X_3+X_3X_4+X_4X_5+X_5X_6+X_6X_1=0,$$
$$X_1X_2X_3+X_2X_3X_4+X_3X_4X_5+X_4X_5X_6+X_5X_6X_1+X_6X_1X_2=0,$$
$$X_1X_2X_3X_4+X_2X_3X_4X_5+X_3X_4X_5X_6+X_4X_5X_6X_1+X_5X_6X_1X_2+X_6X_1X_2X_3=0,$$
$$X_1X_2X_3X_4X_5+X_2X_3X_4X_5X_6+X_3X_4X_5X_6X_1$$
$$+X_4X_5X_6X_1X_2+X_5X_6X_1X_2X_3+X_6X_1X_2X_3X_4=0,$$
$$X_1X_2X_3X_4X_5X_6-1=0.$$

By dehomogenizing through the variable X_4, (S_6) becomes (S_6'):

$$X_1+X_2+X_3+X_5+X_6+1=0,$$
$$X_1X_2+X_2X_3+X_3+X_5+X_5X_6+X_6X_1=0,$$
$$X_1X_2X_3+X_2X_3+X_3X_5+X_5X_6+X_5X_6X_1+X_6X_1X_2=0,$$
$$X_1X_2X_3+X_2X_3X_5+X_3X_5X_6+X_5X_6X_1+X_5X_6X_1X_2+X_6X_1X_2X_3=0,$$
$$X_1X_2X_3X_5+X_2X_3X_5X_6+X_3X_5X_6X_1+X_5X_6X_1X_2+X_5X_6X_1X_2X_3+X_6X_1X_2X_3=0.$$

The permutation group corresponding to (S_6') is $G=\{\mathrm{Id},(2\ 6)(3\ 5)\}$. We choose $L=\{\mathrm{Id},(2\ 6),(3\ 5),(2\ 6)(3\ 5)\}$. Then $G\subset L$, and a system of principal invariants of L is

$$S=X_2+X_6,\quad T=X_3+X_5,\quad P=X_2X_6,\quad Q=X_3X_5,\quad X=X_1.$$

Then, $k[\boldsymbol{X}]^L=k[S,T,P,Q,X]$. The polynomial $\Theta=X_2X_3+X_5X_6$ is a primitive invariant of G relative to L. Its orbit under L is $L.\Theta=\{\Theta,\Theta'\}$, where $\Theta'=X_2X_5+X_3X_6$. So, the equation "H_0" of Theorem 23 is $\Theta^2-(\Theta+\Theta')\Theta+\Theta\Theta'=0$, where

$$\Theta+\Theta'=ST,\quad \Theta\Theta'=Q(S^2-2P)+P(T^2-2Q).$$

So, we compute easily the system (H') of Theorem 23:

$$(S_6'')\begin{cases} S+T+X+1=0,\\ XS+T+\Theta=0,\\ Q+XP+(X+1)\Theta=0,\\ QS+X\Theta+XPT=0,\\ (X+1)PQ+X(QS+PT)=0,\\ \Theta^2-ST\Theta+QS^2+PT^2-4PQ=0. \end{cases}$$

As there is no denominator, Theorem 23 proves that solving (S_6'') will give us exactly the solutions of (S_6'). Now, the 3 first equations in (S_6'') give T, Θ and Q in terms of P, S and X. So, (S_6'') is equivalent to

$$-S-X-1=T,$$
$$S+X+1-XS=\Theta,$$
$$S(X^2-1)-XP-X^2-2X-1=Q,$$
$$(-2XS-X^2-X)P+(X^2-1)S^2-(2X^2+X+1)S+X^2+X=0,$$
$$(X+1)((X^2-X)S^2+((X^2-X-1)P-X^2-X)S$$
$$-XP^2-(X^2+3X+1)P)=0,$$
$$(X^2-X)S^3+((1-X)P-X^2-3X+2)S^2+((6+2X-4X^2)P$$
$$-X^2+2X+3)S+4XP^2+(5P+1)(X+1)^2=0.$$

The fifth equation has two factors; it leads to two different cases. In each one, we eliminate thanks to resultants the remaining variable. We get the following 5 solutions:

(i) $T=1,\ \Theta=-2,\ Q=1,\ P=1,\ S=-1,\ X=-1,$

(ii) $T=-S,\ \Theta=2S,\ Q=1,\ P=1,\ S^2+2S-2=0,\ X=-1,$

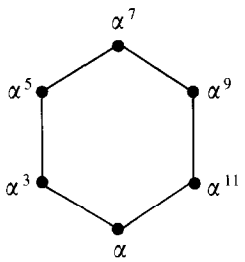
(iii) $T=-S-2,\ \Theta=2,\ Q=-S-3,\ P=S-1,\ S^2+2S-2=0,\ X=1,$

(iv) $T=-X-S-1,\ \Theta=(1-S)X+S+1,\ Q=(1-2S)X-S,\ P=SX+2S+1,$ $S^2+(3-X)S+2X+2=0,\ X^2+4X+1=0,$

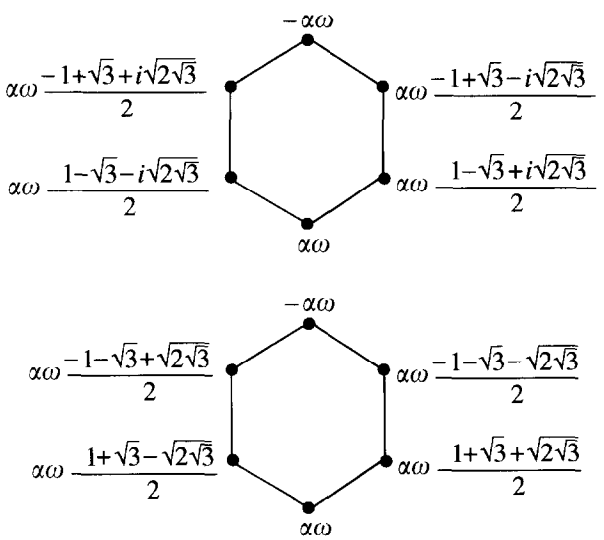
(v) $T=X^3+5X^2-3X-3,\ 2\Theta=X^2+1,\ 4Q=-X^3-5X^2+3X)-1,\ 4P=X^3+3X^2-3X-1,\ 4S=-X^3-5X^2-X-1,\ X^4+4X^3-6X^2+4X+1.$

Now, we study successively these 5 cases.

Case (i). We find the following 12 solutions, where $\alpha=e^{i\pi/6}$.



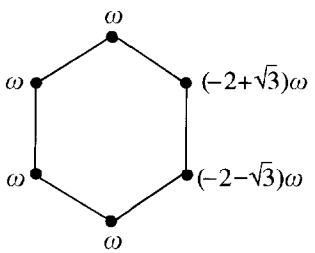
Case (ii). We find 72 solutions partitioned in 2 families:



where we let still $\alpha=(\sqrt{3}+i)/2$, and where ω is one of the elements $1, -j^2=\alpha^2, j=\alpha^4$. We do not let ω run along all the sixth roots of 1, because the 3 other values correspond to the 3 given ones up to a symmetry on the x_i.

Besides, we notice that by permuting circularly the x_i, we find the values of S, T, P, Q, X, Θ corresponding to the case number (v). So, case number (v) yields no other solution.

Case (iii): We find these $12 \times 6 = 72$ solutions, where ω runs along the six sixth roots of unity:



Besides, we notice that by permuting circularly the x_i, we find the values of S, T, P, Q, X, Θ corresponding to the case number (iv).

So, we have found all the solutions of (S_6): we have proved that (S_6) has exactly 156 solutions, written *supra*.

Acknowledgements

The notions of invariant theory that I use here were partially developed in [7]. After the congress AAECC'95, F. Ollivier suggested to me that they could be applied to solve systems like the "cyclic roots systems". Besides, this paper has benefitted from fruitful conversations with M. Chardin, V. Cossart, M. Giusti, D. Lazard, O. Piltant and A. Valibouze. This paper was also enriched thanks to detailed comments, questions and references from the anonymous referees. The author thanks all of them.

References

[1] J.-M. Arnaudiès and A. Valibouze, Lagrange's resolvents, MEGA'96; Rapport Interne LITP 93.63, Univ. Paris 6, December 1993.
[2] AXIOM, The Scientific Computation System, R.D. Jenks and R.S. Sutor (Springer, Berlin 1992).
[3] J. Backelin and R. Fröberg, How we proved that there are exactly 924 cyclic 7-roots, Proc. ISSAC'91 (ACM, New York, 1991) 103–111.
[4] G. Björck and R. Fröberg, A faster way to count the solutions of inhomogeneous systems of algebraic equations, with applications to cyclic n-roots, J. Symbolic Comput. 12 (1991) 329–336.
[5] N. Bourbaki, Éléments de mathématiques (Masson, Paris, 1981).
[6] C. Chevalley, Invariants of finite groups generated by reflections, Amer. J. Math. 77 (1955) 778–782.
[7] A. Colin, Formal computation of Galois groups with relative resolvents, in: G. Cohen, M. Giusti and T. Mora, Eds., Proc. AAECC'95, Lecture Notes in Computer Science, Vol. 948 (Springer, Berlin, 1995) 169–182.
[8] D. Cox, J. Little and D. O'Shea, Ideals, Varieties, and Algorithms (Springer, New York, 1992).
[9] K. Gatermann, Symbolic solution of polynomial equation systems with symmetry, in: S. Watanabe and M. Nagata, Eds., Proc. ISSAC'90 (ACM, New York, 1990).

[10] K. Gatermann, Semi-invariants, equivariants and algorithms, AAECC'7 (Springer, Berlin, 1996) 105–124.
[11] K. Girstmair, On invariant polynomials and their application in field theory, Math. Comput. 48.178 (1987) 781–797.
[12] M. Giusti, D. Lazard and A. Valibouze, Algebraic transformations of polynomial equations, symmetric polynomials and elimination, in: P. Gianni, Ed., ISSAC'88, Lecture. notes in Computer Science, Vol. 358 (Springer, Berlin, 1988) 309–314.
[13] G. Kemper, Das Noethersche Problem und generische Polynome, Dissertation, Univ. of Heidelberg, 1994. Also IWR Preprint 94-49, Heidelberg, 1994.
[14] G. Kemper, Calculating invariant rings of finite groups over arbitrary fields, J. Symbolic Comput. 21 (1996) 351–366.
[15] D. Lazard, Private communication, December 1995.
[16] V.W. Noonburg, A neural network modeled by an adaptive Lotka–Volterra system, SIAM J. Appl. Math. 49 (1989) 1779–1792.
[17] B. Sturmfels, Algorithms in Invariant Theory (Springer, Wien, 1993).
[18] A. Valibouze, SYM, symbolic computation with symmetric polynomials, an extension to Macsyma, in: Proc. Computers and Mathematics (Springer, MIT, Cambridge, MA, 1989) 308–320.
[19] A. Valibouze, Résolvantes et groupe de Galois d'un polynôme, preprint, Paris, 1990.
[20] J. Verschelde and K. Gatermann, Symmetric Newton polytopes for solving sparse polynomial systems, J. Symbolic. Comput. 16 (1995) 95–127.
[21] P.A. Worfolk, Zeros of equivariant vector fields: algorithms for an invariant approach, J. Symbolic Comput. 17 (1994) 487–511.